ESEVEL

ESSENTIAL COMPANY-ISSUED CELL PHONE POLICY TEMPLATE

TABLE OF CONTENT

1. PURPOSE

This policy establishes guidelines for the use of company-issued cell phones to ensure responsible usage, security, and compliance with company regulations. The goal is to support employees in performing their job duties while minimizing risks related to data security, misuse, and cost management.

📌 **Example:**
"The purpose of this policy is to outline **{customize based on company needs, e.g., secure business communication, IT security, cost control}** to ensure that employees use company-issued cell phones responsibly and in compliance with corporate regulations."

2. ELIGIBILITY & ISSUANCE

Company-issued cell phones may be provided to employees based on the following criteria:

- Job role requires frequent business communication (calls, messaging, or video conferencing).
- Need for secure access to corporate apps, systems, and sensitive data.
- On-call responsibilities or support-related tasks requiring 24/7 accessibility.

Device Selection & Procurement:

- Devices will be issued based on company needs and IT department recommendations.
- Employees may request specific models or features, subject to approval.
- Remote employees will receive their devices through the company’s global logistics and procurement partners.

📌 **Example:**

"Company-issued cell phones will be provided to employees in **{list out eligible roles like customer support, IT, and field operations}** roles who require constant connectivity for business tasks.

Employees in eligible roles can submit a request through the IT department, specifying the required device and justification for business use. Approval will be based on job function and business necessity."

💡 ***Useful tip:*** *If your team is distributed across multiple countries, set up a procurement policy that allows local fulfillment and warranty support in different regions.*

3. ACCEPTABLE USE

Company-issued cell phones are intended primarily for business use, including but not limited to:

✓ Business calls, messaging, and video meetings.

✓ Secure access to work applications, company emails, and collaboration tools.

✓ Authentication for work-related systems (e.g., multi-factor authentication apps).

✓ Client communication and customer support.

✓ Emergency work-related situations.

Limited Personal Use

- Personal use should be minimal and must not interfere with work responsibilities.
- Employees must avoid excessive personal calls, streaming, or app usage that results in high data charges.
- Any misuse resulting in additional costs may require reimbursement by the employee.

💡 ***Useful tip:*** *Implement data usage monitoring for remote employees to prevent excessive costs from international roaming or streaming services.*

4. MANDATORY SECURITY MEASURES

🔒 **Device Lock & Authentication:**

- All devices must have strong passwords, biometric authentication, or PIN locks enabled.
- Devices should be auto-locked after a short period of inactivity (recommended: 5 minutes).

💡 ***Useful tip:*** *For remote employees using personal devices for work, enforce company-wide policies requiring multi-factor authentication (MFA) and device encryption to enhance security.*

🔒 **Data Protection & Encryption:**

- Employees must store sensitive business data only on approved company applications.
- Encrypted communication apps (e.g., company-approved messaging tools) must be used for work-related discussions.

🔒 **Mobile Device Management (MDM) Enrollment:**

- All company-issued phones must be registered with the company's MDM system for remote management, security patches, and updates.
- IT reserves the right to enforce security settings, remotely lock or wipe devices in case of loss or non-compliance.

💡 ***Useful tip:*** *Configure MDM policies to automatically enforce updates, disable risky applications, and prevent access from unrecognized locations, reducing the risk of cyber threats for remote workers.*

4. MANDATORY SECURITY MEASURES

🔒 **Lost or Stolen Device Protocol:**

- Employees must report lost, stolen, or compromised devices immediately to IT support.
- IT will initiate remote locking, data wiping, and device tracking where applicable.
- A replacement device will be issued based on approval and company policy.

🔒 **Network & VPN Usage:**

- Employees working remotely must connect via company-approved VPN services when accessing internal systems.
- Public Wi-Fi should be avoided unless using a secured VPN.

💡 ***Useful tip:*** *Implement automatic VPN activation for company-issued devices to ensure that all remote employees connect securely, even if they forget to enable it manually.*

5. PROHIBITED USE

- **Downloading unauthorized apps:** Only pre-approved business applications are allowed.
- **Jailbreaking or rooting devices:** Modifying system settings or bypassing security measures is strictly forbidden.
- **Storing or sharing sensitive data:** Employees should not store business-critical information outside company-approved apps.
- **Engaging in illegal or inappropriate content:** Accessing or sharing offensive, illegal, or explicit content is prohibited.
- **Bypassing security protocols:** Disabling MDM, encryption, or other security settings is a violation of policy.
- **Texting or calling while driving:** Employees must use hands-free devices if required to use their phone while operating a vehicle.

Failure to comply may result in disciplinary action, device revocation, or termination in severe cases.

6. MONITORING & PRIVACY

- The company reserves the right to monitor company-issued cell phones to ensure compliance with security policies and business usage.
- Monitoring may include call logs, messaging activity, installed applications, data usage, and device location (for lost/stolen tracking only).
- Personal data, communications, or private information unrelated to work will not be accessed without the employee's consent.
- Employees should not expect complete privacy when using a company-issued device.

7. RETURN & OFFBOARDING PROCESS

- Employees must return company-issued cell phones upon termination, resignation, or job role change.
- Remote employees must return the device via company-approved shipping services with provided return labels.
- IT will perform a factory reset and data wipe before reassigning the device.
- Employees who fail to return their company-issued device may face:
- Payroll deduction for the cost of the device.
- Legal action in case of non-compliance.

💡 ***Useful tip:*** *Offer an optional buyback program where employees can purchase their company-issued phone at a depreciated cost upon exit.*

8. COST MANAGEMENT & REIMBURSEMENT

Company-Covered Costs

- The company covers standard service plans, including calling, messaging, and data usage for work purposes.
- Work-related international roaming or additional data requirements must be pre-approved.

Employee Responsibilities

- Employees may be responsible for excessive personal use fees, premium services, or unauthorized subscriptions.
- Reimbursement for business-related personal device usage (if applicable) must be pre-approved and claimed through expense reports.

9. VIOLATIONS & DISCIPLINARY ACTIONS

Failure to comply with this policy may result in:

- ⚠ **First Violation:** Formal warning and mandatory training on policy compliance.
- ⚠ **Second Violation:** Revocation of company-issued device privileges.
- ⚠ **Severe Violations:** Possible termination or legal action if there is a breach of security, financial loss, or misuse of company property

ESEVEL

Esevel provides a full-stack IT management platform streamlining cell phone procurement, security, and support across Asia Pacific.

- ✓ **Seamless device procurement & deployment** – Easily source, configure, and deliver to employees across 88+ countries.
- ✓ **Centralized device management** – Track, manage, and secure with real-time monitoring and automated provisioning.
- ✓ **Robust security & compliance –** Enable remote locking and wiping and ensure compliance with corporate IT standards.
- ✓ **Automated onboarding & offboarding –** Provision and de-provision devices effortlessly
- ✓ **24/5 it support & repairs –** Get real-time IT support and global repair services to keep your operation running.

Book a demo now →